

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Masahiro SUEYOSHI, et al.

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: HERewith

FOR: DATA PROCESSING DEVICE AND METHOD AND PROGRAM OF SAME

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number _____, filed _____, is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e):
Application No. _____ Date Filed _____
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

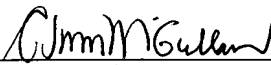
<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2003-070301	March 14, 2003

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. _____ filed _____
- ☐ were submitted to the International Bureau in PCT Application Number _____
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. _____ filed _____; and
- ☐ (B) Application Serial No.(s) _____
☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.


Bradley D. Lytle

Registration No. 40,073

C. Irvin McClelland
Registration Number 21,124

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 3 月 1 4 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 0 7 0 3 0 1
Application Number:

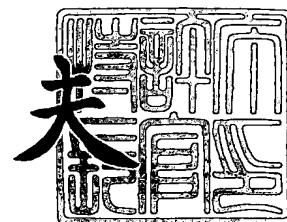
[ST. 10/C] : [J P 2 0 0 3 - 0 7 0 3 0 1]

出 願 人 ソニー株式会社
Applicant(s):

2 0 0 3 年 1 2 月 1 0 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 0390086803

【提出日】 平成15年 3月14日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 7/00

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 末吉 正弘

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 舘野 啓

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 平野 義昭

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 照山 勝幸

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100094053

【弁理士】

【氏名又は名称】 佐藤 隆久

【手数料の表示】

【予納台帳番号】 014890

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707389

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ処理装置、その方法およびそのプログラム

【特許請求の範囲】

【請求項 1】

鍵データを基に認証先との間で認証を行う認証手段と、
前記認証手段から受けたデータを基に前記鍵データを生成して前記認証手段に
提供する鍵生成手段と
を有し、
前記認証手段は、第 1 のデータと第 2 のデータとを前記鍵生成手段に提供し、
前記鍵生成手段は、前記認証手段から受けた前記第 1 のデータと前記第 2 のデ
ータとのうち前記第 1 のデータのみを用いて前記鍵データを生成する
データ処理装置。

【請求項 2】

前記鍵生成手段は、前記認証手段から受けたデータを基に、当該認証先に固有
の前記鍵データを生成する
請求項 1 に記載のデータ処理装置。

【請求項 3】

前記鍵生成手段は、第 1 の入力パラメータおよび第 2 の入力パラメータを持ち
、前記第 1 の入力パラメータに代入された前記第 1 のデータのみを用いて前記鍵
データを生成する機能モジュールを備え、
前記認証手段は、前記鍵生成手段の前記機能モジュールの前記第 1 の入力パラ
メータに前記第 1 のデータを代入し、前記第 2 の入力パラメータに前記第 2 のデ
ータを代入する
請求項 1 に記載のデータ処理装置。

【請求項 4】

前記認証手段は、前記認証の後に行う処理に関する識別データであり前記認証
先から受けた前記第 1 のデータおよび前記第 2 のデータを前記鍵生成手段に提供
する
請求項 1 に記載のデータ処理装置。

【請求項 5】

前記認証手段は、前記認証先から受けた当該認証先に固有の固有データを提供する処理を行う機能モジュールを備え、

前記鍵生成手段は、前記認証手段の前記機能モジュールを呼び出し、当該機能モジュールから受けた前記固有データをさらに用いて、前記鍵データを生成する請求項 1 に記載のデータ処理装置。

【請求項 6】

前記認証手段は、前記機能モジュールを規定する関数を含む認証プログラムを実行手段で実行して実現され、

前記鍵生成手段は、前記機能モジュールの呼び出し手順を含む鍵生成プログラムを前記実行手段で実行して実現される

請求項 5 に記載のデータ処理装置。

【請求項 7】

前記認証手段は、前記鍵生成手段によって前記機能モジュールが呼び出されると、当該機能モジュールの実行に応じて、前記認証手段と前記鍵生成手段とで共用される記憶手段から読み出した前記固有データを前記鍵生成手段に提供する

請求項 5 に記載のデータ処理装置。

【請求項 8】

マスタ鍵データを読み出す機能モジュールを備え、前記マスタ鍵データを保持する鍵保持手段

をさらに有し、

前記鍵生成手段は、前記鍵保持手段の前記機能モジュールを呼び出し、当該機能モジュールが取り出した前記マスタ鍵データをさらに用いて前記鍵データを生成する

請求項 1 に記載のデータ処理装置。

【請求項 9】

前記鍵保持手段は、鍵保持プログラムを実行手段で実行して実現される

請求項 8 に記載のデータ処理装置。

【請求項 10】

前記鍵保持プログラムは、前記認証手段および前記鍵生成手段を実現するプログラムとは独立して更新される

請求項 9 に記載のデータ処理装置。

【請求項 1 1】

前記鍵生成手段は、前記認証の後に行われる複数の処理内容のそれぞれに対応して規定された異なる複数の鍵生成アルゴリズムのうち、指定された処理内容に対応した前記鍵生成アルゴリズムを選択し、当該選択した鍵生成アルゴリズムを基に、当該認証先に固有の前記鍵データを生成する

請求項 1 に記載のデータ処理装置。

【請求項 1 2】

前記認証手段は、前記鍵データを基に前記認証先との間の認証を行い、前記認証先との間で互いの正当性を認めると、前記鍵データに対応付けられた処理を前記認証先と連携して行う

請求項 1 に記載のデータ処理装置。

【請求項 1 3】

前記鍵生成手段は、前記認証先に固有の前記第 1 のデータを基に当該認証先に固有の個別鍵データを生成し、

前記認証手段は、当該認証手段が保持する複数の前記認証先で共用される固定鍵データを用いて前記認証先との間で第 1 の認証を行い、前記鍵生成手段が生成した前記個別鍵データを用いて前記認証先との間で第 2 の認証を行う

請求項 1 に記載のデータ処理装置。

【請求項 1 4】

前記認証手段は、前記第 1 の認証により前記認証先の正当性を確認した後に前記認証先と連携して前記固定鍵データに対応付けられた第 1 の処理を行い、前記第 2 の認証により前記認証先の正当性を確認した後に前記認証先と連携して前記個別鍵データに対応付けられた第 2 の処理を行う

請求項 1 3 に記載のデータ処理装置。

【請求項 1 5】

前記認証手段は、前記第 2 の認証に関連付けられた原鍵データを保持し、

前記鍵生成手段は、前記認証手段を介して前記認証先から受けた固有データと前記認証手段が保持する前記原鍵データとを基に、前記個別鍵データを生成する請求項 1 3 に記載のデータ処理装置。

【請求項 1 6】

前記認証手段は、前記認証先との間で行われる処理の識別データを、前記原鍵データと対応付けて保持し、指定された処理の前記識別データに対応付けられた前記原鍵データを前記鍵生成手段に提供し、

前記鍵生成手段は、前記認証手段が受けた前記原鍵データを基に前記個別鍵データを生成する

請求項 1 5 に記載のデータ処理装置。

【請求項 1 7】

鍵生成手段が生成した鍵データを基に認証手段が認証先との間で認証を行うデータ処理方法であって、

前記認証手段が、前記鍵生成手段に第 1 のデータと第 2 のデータとを提供する第 1 の工程と、

前記鍵生成手段が、前記第 1 の工程で得た前記第 1 のデータおよび前記第 2 のデータのうち前記第 1 のデータのみを用いて鍵データを生成し、当該鍵データを前記認証手段に提供する第 2 の工程と、

前記認証手段が、前記第 2 の工程で受けた前記鍵データを基に認証先と認証を行う第 3 の工程と

を有するデータ処理方法。

【請求項 1 8】

前記第 2 の工程において、前記鍵生成手段が、前記第 1 の工程で前記認証手段から受けたデータを基に、当該認証先に固有の前記鍵データを生成する

請求項 1 7 に記載のデータ処理方法。

【請求項 1 9】

前記第 2 の工程において、前記鍵生成手段が、第 1 の入力パラメータおよび第 2 の入力パラメータを持つ機能モジュールを基に、当該機能モジュールの前記第 1 の入力パラメータに代入された前記第 1 のデータのみを用いて前記鍵データを

生成し、

前記第 1 の工程において、前記認証手段が、前記鍵生成手段の前記機能モジュールの前記第 1 の入力パラメータに前記第 1 のデータを代入し、前記第 2 の入力パラメータに前記第 2 のデータを代入する

請求項 17 に記載のデータ処理方法。

【請求項 20】

前記第 2 の工程において、前記鍵生成手段が、前記認証手段の機能モジュールを呼び出し、当該機能モジュールを基に得た前記認証先に固有の固有データをさらに用いて前記鍵データを生成する

請求項 17 に記載のデータ処理方法。

【請求項 21】

前記第 2 の工程において、前記鍵生成手段が、鍵保持手段の機能モジュールを呼び出し、当該機能モジュールから得られた前記鍵保持手段が保持する前記マスター鍵データをさらに用いて前記鍵データを生成する

請求項 17 に記載のデータ処理方法。

【請求項 22】

前記鍵保持手段を実現する鍵保持プログラムを、前記認証手段および前記鍵生成手段を実現するプログラムとは独立して更新する第 4 の工程

をさらに有する請求項 21 に記載のデータ処理方法。

【請求項 23】

鍵データを基に認証先と認証を行う手順を記述した認証プログラムに対して前記鍵データを提供する手順を記述し、データ処理装置で実行されるプログラムであって、

前記認証プログラムから第 1 のデータと第 2 のデータとを受ける第 1 の手順と、

、

前記第 1 の手順で受けた前記第 1 のデータと前記第 2 のデータとのうち前記第 1 のデータのみを用いて前記鍵データを生成する第 2 の手順と、

前記第 2 の手順で生成した前記鍵データを前記認証プログラムに提供する第 3 の手順と

の記述を有するプログラム。

【請求項 24】

前記第 2 の手順は、前記第 1 の手順で受けた前記第 1 のデータを基に、当該認証先に固有の前記鍵データを生成する

請求項 23 に記載のプログラム。

【請求項 25】

第 1 の入力パラメータおよび第 2 の入力パラメータを持ち、前記第 1 の入力パラメータに代入された前記第 1 のデータのみを用いて前記鍵データを生成する手順を示す関数

をさらに有し、

前記第 1 の手順は、前記関数の前記第 1 の入力パラメータおよび前記第 2 の入力パラメータを介してそれぞれ前記第 1 のデータおよび前記第 2 のデータを受け

前記第 2 の手順は、前記関数の前記第 1 の入力パラメータを介して受けた前記第 1 のデータのみを用いて前記鍵データを生成する

請求項 23 に記載のプログラム。

【請求項 26】

前記認証プログラムとは異なるアクセス権限が規定されている

請求項 23 に記載のプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、認証先との間で鍵データを用いた認証を行うデータ処理装置、その方法およびプログラムに関する。

【0002】

【従来の技術】

例えば、鍵データを基に認証先と認証を行い、認証により相手の正当性を確認した後に種々の処理を行うデータ処理装置がある。

このようなデータ処理装置には、例えば、鍵データを基にした認証を行う認証

機能と、上記鍵データを生成する鍵生成機能とがある。

従来のデータ処理装置は、上記認証機能と鍵生成機能とが混在して構成されている。

【0003】

【発明が解決しようとする課題】

上述した従来のデータ処理装置では、認証機能と鍵生成機能とを異なる開発者が開発させ、鍵生成機能が使用する鍵生成アルゴリズムを、認証機能の開発者に対して秘密にしたいという要請がある。

しかしながら、上述した従来のデータ処理装置では、認証機能と鍵生成機能とが混在しているため、上述した要請に応えることが困難であるという問題がある。

【0004】

本発明はかかる事情に鑑みてなされたものであり、その目的は、鍵生成手段における鍵データの生成手法を認証手段の開発者に秘密にできるデータ処理装置、その方法およびそのプログラムを提供することを目的とする。

【0005】

【課題を解決するための手段】

上記の目的を達成するため、第1の発明のデータ処理装置は、鍵データを基に認証先との間で認証を行う認証手段と、前記認証手段から受けたデータを基に前記鍵データを生成して前記認証手段に提供する鍵生成手段とを有し、前記認証手段は、第1のデータと第2のデータとを前記鍵生成手段に提供し、前記鍵生成手段は、前記認証手段から受けた前記第1のデータと前記第2のデータとのうち前記第1のデータのみを用いて前記鍵データを生成する。

【0006】

第1の発明のデータ処理装置の作用は以下のようになる。

認証手段が、第1のデータと第2のデータとを前記鍵生成手段に提供する。

そして、鍵生成手段が、前記認証手段から受けた前記第1のデータと前記第2のデータとのうち前記第1のデータのみを用いて前記鍵データを生成する。

そして、認証手段が、前記鍵生成手段が生成した前記鍵データを基に認証先と

認証を行う。

【0007】

また、第1の発明のデータ処理装置は、好ましくは、前記鍵生成手段は、前記認証手段から受けたデータを基に、当該認証先に固有の前記鍵データを生成する。

また、第1の発明のデータ処理装置は、好ましくは、前記鍵生成手段は、第1の入力パラメータおよび第2の入力パラメータを持ち、前記第1の入力パラメータに代入された前記第1のデータのみを用いて前記鍵データを生成する機能モジュールを備え、前記認証手段は、前記鍵生成手段の前記機能モジュールの前記第1の入力パラメータに前記第1のデータを代入し、前記第2の入力パラメータに前記第2のデータを代入する。

【0008】

第2の発明のデータ処理方法は、鍵生成手段が生成した鍵データを基に認証手段が認証先との間で認証を行うデータ処理方法であって、前記認証手段が、前記鍵生成手段に第1のデータと第2のデータとを提供する第1の工程と、前記鍵生成手段が、前記第1の工程で得た前記第1のデータおよび前記第2のデータのうち前記第1のデータのみを用いて鍵データを生成し、当該鍵データを前記認証手段に提供する第2の工程と、前記認証手段が、前記第2の工程で受けた前記鍵データを基に認証先と認証を行う第3の工程とを有する。

【0009】

第3の発明のプログラムは、鍵データを基に認証先と認証を行う手順を記述した認証プログラムに対して前記鍵データを提供する手順を記述し、データ処理装置で実行されるプログラムであって、前記認証プログラムから第1のデータと第2のデータとを受ける第1の手順と、前記第1の手順で受けた前記第1のデータと前記第2のデータとのうち前記第1のデータのみを用いて前記鍵データを生成する第2の手順と、前記第2の手順で生成した前記鍵データを前記認証プログラムに提供する第3の手順との記述を有する。

【0010】

【発明の実施の形態】

以下、本発明の実施形態に係わるカードシステムについて説明する。

図1は、本実施形態のカードシステム1の構成図である。

図1に示すように、カードシステム1は、例えば、R/W(Reader/Writer) 11を介してICカード10のIC(Integrated Circuit) 15とSAM(Secure Application Module) 12とが認証を行った後に、連携して所定のサービスに関する処理を行う。

ここで、SAM12が本発明のデータ処理装置に対応し、IC15が本発明の認証先に対応している。

また、管理装置13は、SAM12とIC15の間の相互認証に用いられる鍵データ等を格納した鍵パッケージKPをSAM12に登録する。

また、SAM12の管理者、例えば、ICカード10を利用した所定のサービスの提供者は、複数のユーザの各々にICカード10を発行する。

【0011】

IC15は、後述するように、SAM12を利用してIC15のユーザが受ける種々のサービスに関するデータおよびプログラムのファイルデータを記憶しており、当該ファイルデータを用いたサービスに利用権限が設定されている。具体的には、IC15とSAM12とが指定されたサービスに対応付けられた鍵データを基に相互認証を行い、お互いの正当性を確認したことを条件に、IC15とSAM12とが連携して上記サービスに係わる処理を行う。

本実施形態では、上記複数のユーザの各々に発行されたICカード10には、上記認証に用いられる鍵データの一部として、個々のICカード10に固有の鍵データ（本発明の鍵データまたは個別鍵データ）が割り当てられている。

そして、SAM12は、ICカード10から、当該ICカード10の固有データ、例えば、製造時にICカード10に固有に割り当てられたシリアル番号などの装置識別データIDMと、指定されたサービス等を識別する複数の識別データSID1、SID2、SID3とを入力し、これらを基に所定のアルゴリズムで認証に用いる上記鍵データを生成する。

【0012】

以下、図1に示す各構成要素について説明する。

〔 I C 1 5 〕

図 2 は、図 1 に示す I C カード 1 0 に内蔵された I C 1 5 の構成図である。

図 2 に示すように、 I C 1 5 は、例えば、インタフェース 2 1、メモリ 2 2 および C P U 2 3 を有し、これらが内部バス 2 0 を介して接続されている。

インタフェース 2 1 は、 R / W 1 1 を介して S A M 1 2 との間でデータの授受を行う。

メモリ 2 2 は、 S A M 1 2 を利用して I C 1 5 のユーザが受ける種々のサービスに関する処理に用いられるデータおよびプログラムのファイルデータを記憶している。

また、メモリ 2 2 は、上記サービスに関する処理を行う前に S A M 1 2 との間の認証に用いられる種々の鍵データを記憶している。

また、メモリ 2 2 は、個々の I C カード 1 0 に固有の装置識別データ I D M を記憶している。

【 0 0 1 3 】

なお、 S A M 1 2 は、例えば、同じ機種種の S A M 1 2 に共通して割り当てられたシステムコードに対応付けられた鍵データを基に相互認証を行い、当該相互認証により互いの正当性が認められたことを条件に、 I C 1 5 に対してのアクセスが許可される。

さらに、メモリ 2 2 内で種々のサービスのファイルデータは、それぞれ階層構造を有するフォルダであるエリア内に格納されている。

S A M 1 2 は、メモリ 2 2 内のエリアのエリアコードに対応付けられた鍵データを基に相互認証を行い、当該相互認証により互いの正当性が認められたことを条件に、当該エリアに対してのアクセスが許可される。

さらに、 S A M 1 2 は、エリア内に記憶されたファイルデータのサービスコードに対応付けられた鍵データを基に相互認証を行い、当該相互認証により互いの正当性が認められたことを条件に、当該ファイルデータに対してのアクセスが許可される。

【 0 0 1 4 】

本実施形態では、図 3 に示すように、 I C 1 5 に関して上述したように規定さ

れた鍵データの種類には、固定鍵データと個別鍵データとが規定されている。

固定鍵データは、例えば、複数の IC カード 10 の IC 15 の間で、ファイルシステム上の位置が同一であれば、その値が同じである鍵データである。すなわち、固定鍵データは、複数の IC カード 10 の IC 15 で共用される鍵データである。

個別鍵データは、複数の IC カード 10 の IC 15 の間で、ファイルシステム上の位置が同一であっても、その値が異なる鍵データである。すなわち、個別鍵データは、複数の IC カード 10 の IC 15 の各々で固有の鍵データである。

なお、IC 15 は、上記鍵データが固定鍵データおよび個別鍵データのいずれであるかを特定することなく処理を行う。

【0015】

CPU 23 は、メモリ 22 から読み出したプログラム、並びに鍵データを基に、インタフェース 21 および R/W 11 を介して、SAM 12 とデータの授受を行って SAM 12 と相互認証を行う。

また、CPU 23 は、上記相互認証で互いの正当性を確認すると、SAM 12 と連携して、相互認証で用いた鍵データに対応付けられたサービスに関する処理を実行する。

また、CPU 23 は、例えば、IC カード 10 の発行時に、所定の権限が認証された管理者の操作に応じて、インタフェース 21 を介して暗号化された鍵パッケージを復号し、当該復号した鍵パッケージ内の上記鍵データをメモリ 22 に書き込む。

【0016】

〔SAM 12〕

図 4 は図 1 に示す SAM 12 の機能ブロック図、図 5 は認証時における SAM 12 のデータの流れを説明するための図、図 6 は SAM 12 のソフトウェア構成を説明するための図である。

図 4 に示すように、SAM 12 は、例えば、インタフェース 31、カード処理部 32、鍵管理部 33、鍵生成部 34 および鍵保存部 35 を有し、これらが内部バス 30 を介して接続されている。

本実施形態において、カード処理部 32 および鍵管理部 33 が本発明の認証手段に対応し、鍵生成部 34 が本発明の鍵生成手段に対応し、鍵保存部 35 が本発明の鍵保持手段に対応している。

【0017】

また、図 6 に示すように、カード処理部 32 および鍵管理部 33 は、認証プログラム 80（本発明の認証プログラム）を CPU（図示しない）などのデータ処理装置（本発明の実行手段またはデータ処理装置）で実行して実現される。

また、鍵生成部 34 は、鍵生成プログラム 81（本発明のプログラムまたは鍵生成プログラム）を上記 CPU などのデータ処理装置で実行して実現される。

また、鍵保存部 35 は、鍵保存プログラム 82（本発明の鍵保存プログラム）を上記 CPU などのデータ処理装置で実行して実現される。

【0018】

本実施形態では、図 7 に示すように、認証プログラム 80 にファイアウォール FW1 が規定され、鍵生成プログラム 81 および鍵保存プログラム 82 にファイアウォール FW2 が規定されている。

すなわち、ファイアウォール FW1, FW2 により、鍵生成プログラム 81 および鍵保存プログラム 82 へのアクセス権限は、認証プログラム 80 へのアクセス権限とは別に規定されている。

具体的には、SAM12 内において、鍵生成プログラム 81 および鍵保存プログラム 82 が記憶された記憶領域へのアクセス権限は、認証プログラム 80 が記憶された記憶領域へのアクセス権限とは別に規定されている。

従って、認証プログラム 80 へのアクセス権限を有する者でも、認証プログラム 80 および鍵生成プログラム 81 へのアクセス権限を有しない場合には、認証プログラム 80 および鍵生成プログラム 81 へのアクセスは禁止される。

また、鍵保存プログラム 82 は、鍵生成プログラム 81 および認証プログラム 80 のダウンロードとは独立して、SAM12 の外部からダウンロードされる。

【0019】

また、本実施形態では、認証プログラム 80 から鍵生成プログラム 81 に、IC15 の装置識別データ IDM と、サービス等の複数の識別データ SID1, S

ID 2, SID 3 を提供する。

そして、鍵生成プログラム 81 は、認証プログラム 80 から入力した上記データのうち、装置識別データ IDM と識別データ SID 2 (本発明の第 1 のデータ) とを基に、個別鍵データ KI (本発明の鍵データ) を生成する。すなわち、鍵生成プログラム 81 は、認証プログラム 80 から入力した識別データ SID 1, SID 3 (本発明の第 2 のデータ) を、個別鍵データ KI の生成に用いない。

【0020】

以下、鍵生成プログラム 81 と、認証プログラム 80 および鍵保存プログラム 82 との間でのデータの授受の手法を説明する。

本実施形態では、図 6 に示すように、認証プログラム 80 は、鍵生成プログラム 81 内の API (Application Program Interface) 関数である関数 API 1 を呼び出し、下記式 (1) に示すように、当該関数 API 1 の入力パラメータとして、IC カードの IC 5 から入力したサービス等の識別データ SID 1, 2, 3 を代入する記述 (コード) を有する。

【0021】

【数 1】

API 1 (SID 1, SID 2, SID 3) ... (1)

【0022】

そして、認証プログラム 80 を基にした当該コードの実行に応じて、識別データ SID 1, 2, 3 が、指定されたバッファ (図示せず) 内のアドレスに書き込まれる。そして、鍵生成プログラム 81 内の関数 API 1 の実行に応じて、上記アドレスに書き込まれた識別データ SID 1, 2, 3 を入力パラメータとして用いて鍵生成が行われる。なお、鍵生成プログラム 81 は、上記 API 関数の実行の戻り値として受けた上記バッファ内のアドレスに、識別データ SID 1, 2, 3 を書き込んでもよい。

なお、認証プログラム 80 から鍵生成プログラム 81 への原鍵データ KO の提供も、上記 API 1 関数を介して行われる。

上述したように、SAM 12 は、鍵生成プログラム 81 で規定された API 1 関数を介して、認証プログラム 80 から鍵生成プログラム 81 に、識別データ S

ID1～SID3 および原鍵データ KO を提供する。

【0023】

また、認証プログラム 80 は、関数 API2 を有し、IC カードの IC5 から入力した装置識別データ IDM を関数 API2 の戻り値として規定されたバッファ内のアドレスに格納する。

そして、鍵生成プログラム 81 が、関数 API2 を呼び出し、その戻り値として規定されたアドレスから、装置識別データ IDM を読み出す。

上述したように、SAM12 は、認証プログラム 80 で規定された関数 API2 を介して、認証プログラム 80 から鍵生成プログラム 81 に装置識別データ IDM を提供する。

【0024】

また、鍵保存プログラム 82 は、関数 API3 を有し、鍵保存プログラム 82 が保持するマスタ鍵データ KM を、関数 API3 の戻り値として規定されたバッファ内のアドレスに格納する。

そして、鍵生成プログラム 81 が、関数 API3 を呼び出し、その戻り値として規定されたアドレスから、マスタ鍵データ KM を読み出す。

上述したように、SAM12 は、鍵保存プログラム 82 で規定された関数 API3 を介して、鍵保存プログラム 82 から鍵生成プログラム 81 にマスタ鍵データ KM を提供する。

【0025】

なお、関数 API1, API2, API3 が本発明の機能モジュールに対応している。

【0026】

以下、SAM12 の構成要素について説明する。

インタフェース 31 は、図 1 に示す R/W11 を介して IC15 との間でデータ授受を行う。

カード処理部 32 は、鍵管理部 33 から入力した鍵データを基に、インタフェース 31 を介して IC カード 10 の IC15 と相互認証を行い、当該相互認証により互いの正当性を確認すると、指定されたサービスに関する処理を IC15 と

連携して行う。カード処理部 32 は、アプリケーションプログラムを実行することで種々の機能を実現する。

カード処理部 32 は、鍵管理部 33 から入力した鍵データを基に IC15 との間で相互認証を行う。

【0027】

鍵管理部 33 は、上記相互認証等に用いる鍵データを管理する鍵管理データ KMD を保持している。

鍵管理データ KMD は、図 5 に示すように、識別データ SID と、鍵データ K と、鍵特性データ KPD とを対応付けて示している。

識別データ SID は、SAM12 が IC15 と連携して行うサービス（ファイルデータ）および当該サービスに伴って IC15 にアクセスする記憶領域（フォルダ）等を識別するデータである。識別データ SID は、例えば、IC15 から入力したシステムコード、エリアコードあるいはサービスコードである。

本実施形態では、図 6 に示すように、認証プログラム 80 が、IC カードの IC5 から入力した装置識別データ IDM と、サービス等の識別データ SID1, 2, 3 を鍵生成プログラム 81 に提供する。

【0028】

鍵データ K は、上記サービスに先立って行う IC15 との間の相互認証に用いる鍵データである。なお、個別鍵データを基に行われる処理の識別データ SID には、鍵データ K として前述した原鍵データ KO が関連付けられている。

鍵特性データ KPD は、鍵データ K が前述した固定鍵データおよび個別鍵データの何れであることを示すデータである。

【0029】

鍵管理部 33 は、鍵管理データ KMD の鍵特性データ KPD を基に、カード処理部 32 からの鍵要求 KREQ 内の識別データ SID が固定鍵データに対応付けられている場合には、鍵管理データ KMD から当該識別データ SID に対応する鍵データ（固定鍵データ）K を読み出してカード処理部 32 に出力する。

一方、鍵管理部 33 は、鍵管理データ KMD の鍵特性データ KPD を基に、カード処理部 32 からの鍵要求 KREQ 内の識別データ SID が個別鍵データに対

応付けられている場合には、カード処理部 32 に装置識別データ IDM を要求し（図 5 中の要求 IDM_REQ）、それに応じて入力した装置識別データ IDM と、識別データ SID と、鍵管理データ KMD から取り出した当該識別データ SID に対応する鍵データ K（図 5 原中の鍵データ KO）とを鍵生成部 34 に出力する。当該識別データ SID および原鍵データ KO は、前述したように、関数 API1 を介して、認証プログラム 80 から鍵生成プログラム 81 に提供される。

【0030】

鍵管理部 33 への鍵管理データ KMD の設定は、例えば、以下のように行われる。

すなわち、図 1 に示す管理装置 13 が、図 8 に示すように、鍵管理データ KMD を設定用マスタ鍵データ KPM で暗号化した鍵パッケージデータ KP を生成し、これを SAM12 に出力する。

SAM12 は、インタフェース 31 を介して入力した鍵パッケージデータ KP を、図 4 に示す鍵管理部 33 あるいは図示しない復号部において、設定用マスタ鍵データ KPM を用いて復号して鍵管理データ KMD を生成し、これを保持する。

ここで、鍵管理部 33 への鍵管理データ KMD の設定を SAM12 を用いたサービスを提供する事業者が行うようにすることで、当該事業者が鍵管理をセキュアな状態で、しかも高い自由度で行うことができる。

なお、鍵管理データ KMD 内に格納された個別鍵の生成原となる鍵データ KO は、個別鍵データ KI そのものではないので、鍵管理データ KMD の秘匿性が失われた場合でも、個別鍵データ KI 自体の秘匿性は失われない。

【0031】

鍵生成部 34 は、鍵保存部 35 からのマスタ鍵データ KM と、鍵管理部 33 から入力した装置識別データ IDM と、識別データ SID と、鍵データ K（KO）とを基に、個別鍵生成プログラム KPRG を実行して鍵データ（個別鍵データ）KI を生成し、これを鍵管理部 33 に出力する。

鍵管理部 33 は、鍵生成部 34 から入力した鍵データ KI をカード処理部 32 に出力する。

鍵生成部 34 は、例えば、図 9 に示す手順で鍵データ K I を生成する。

図 9 に示す各手順は、個別鍵生成プログラム K P R G に記述されている。

以下、図 9 に示す各ステップを説明する。

ステップ S T 1 1 :

鍵生成部 34 は、前述したように鍵生成プログラム 81 で規定された関数 A P I 1 を基に、識別データ S I D 1, S I D 2, S I D 3 と、原鍵データ K O を鍵管理部 33 から入力する。

ステップ S T 1 2 :

鍵生成部 34 は、前述したように認証プログラム 80 で規定された関数 A P I 2 を基に、装置識別データ I D M を鍵管理部 33 から入力する。

ステップ S T 1 3 :

鍵生成部 34 は、前述したように鍵保存プログラム 82 で規定された関数 A P I 3 を基に、マスタ鍵データ K M を鍵保存部 35 から入力する。

ステップ S T 1 4 :

鍵生成部 34 は、ステップ S T 1 1 で入力した識別データ S I D 2 と、ステップ S T 1 2 で入力した装置識別データ I D M と、ステップ S T 1 3 で入力したマスタ鍵データ K M とを加算してデータ X を生成する。

このように、鍵生成部 34 では、ステップ S T 1 1 で入力した識別データ S I D 1, S I D 2, S I D 3 のうち識別データ S I D 2 をデータ X の生成に用い、識別データ S I D 1, S I D 3 をデータ X の生成に用いない。これにより、カード処理部 32 および鍵管理部 33 を規定する認証プログラム 80 から、鍵生成プログラム 81 の処理を秘密にできる。

ステップ S T 1 5 :

鍵生成部 34 は、ステップ S T 1 1 で入力した原鍵データ K O を、ステップ S T 1 4 で生成したデータ X の値分だけ右をローテートシフトして個別鍵データ K I を生成する。

ステップ S T 1 6 :

鍵生成部 34 は、ステップ S T 1 3 で生成した個別鍵データ K I を鍵管理部 33 に出力する。

【0032】

なお、鍵生成部34が鍵データKIの生成に用いる個別鍵生成プログラムKPRGとして、例えば、IC15との間の処理内容毎、例えば処理対象のファイルシステム上での位置毎、例えばエリアコード毎に異なるアルゴリズムのプログラムを用意し、指定された識別データSID2に対応するプログラムを選択して実行してもよい。

また、鍵生成部34は、マスタ鍵データKMを用いずに個別鍵データKIを生成してもよい。

また、個別鍵データの図7に示す生成手順は一例であり、本発明はこれに限定されるものではない。

【0033】

このように、鍵生成部34では、マスタ鍵データKMの他に、装置識別データIDMと、識別データSIDと、鍵データK(KO)とを用いて個別鍵データを生成することで、これらのデータに鍵生成に関してマスタ鍵データと同等の役割を持たせることができる。そのため、鍵管理データKMDの設定に関する権限を有する事業者等が認証に用いる鍵データに関する設定を自由に変更させることができる。

また、上述したように、ファイルシステム上での位置等を基に、個別鍵生成プログラムKPRGが異なるアルゴリズムを基に個別鍵データを生成することで、よりセキュリティを高めることができる。すなわち、一部のエリア・サービス用のロジックが漏洩した場合でも、他のエリア・サービスのセキュリティを保つことができる。

【0034】

以下、図1に示すカードシステム1の動作例を説明する。

〔第1の動作例〕

当該動作例では、SAM12に鍵管理データKMDを設定する場合を説明する。

図10は、当該動作例を説明するためのフローチャートである。

ステップST21：

図1に示す管理装置13が、図6に示すように、鍵管理データKMDを設定用マスタ鍵データKPMで暗号化した鍵パッケージデータKPを生成し、これをSAM12に出力する。

ステップST22：

SAM12は、インタフェース31を介して入力した鍵パッケージデータKPを、図4に示す鍵管理部33あるいは図示しない復号部において、設定用マスタ鍵データKPMを用いて復号して鍵管理データKMDを生成する。

ステップST23：

鍵管理部33は、ステップST22で生成した鍵管理データKMDを保持する。

【0035】

〔第2の動作例〕

当該動作例では、図5を基にICカード10bのIC15と、SAM12との間でサービスに関する処理を行う場合の動作例を説明する。

図11および図12は、当該動作例を説明するためのフローチャートである。

ステップST31：

ユーザが図1に示すR/W11にICカード10を装着し、例えば、R/W11に設けられた操作部を用いて自らが希望するサービスを指定する。なお、当該サービスの指定は、IC15あるいはSAM12が自動的に行ってもよい。

これにより、IC15からSAM12に、指定されたサービスの識別データSIDと、IC15のメモリ22から読み出された装置識別データIDMとがSAM12に出力される。

【0036】

ステップST32：

カード処理部32は、ステップST31で入力した識別データSIDを含む鍵要求KREQを鍵管理部33に出力する。

ステップST33：

鍵管理部33は、鍵管理データKMDを参照し、ステップST22で入力した鍵要求KREQに含まれる識別データSIDに対応付けられた鍵データKが、個

別鍵および固定鍵の何れであることを特定する。

ステップ S T 3 4 :

鍵管理部 3 3 は、ステップ S T 3 3 で固定鍵であると特定した場合にステップ S T 3 5 に進み、個別鍵であると特定した場合にステップ S T 3 8 に進む。

【 0 0 3 7 】

ステップ S T 3 5 :

鍵管理部 3 3 は、鍵管理データ KMD を参照して、ステップ S T 3 2 で入力した識別データ S I D に対応する鍵データ（固定鍵データ）を得る。

ステップ S T 3 6 :

鍵管理部 3 3 は、ステップ S T 3 5 で得た鍵データ、あるいは後述するステップ S T 4 2 で鍵生成部 3 4 から入力した鍵データをカード処理部 3 2 に出力する。

【 0 0 3 8 】

ステップ S T 3 7 :

カード処理部 3 2 は、ステップ S T 3 6 で入力した鍵データを基に、I C 1 5 との間で相互認証を行い、互いの正当性を確認すると、ステップ S T 3 1 で入力した識別データ S I D に対応するサービス処理を I C 1 5 と連携して行う。

【 0 0 3 9 】

ステップ S T 3 8 :

鍵管理部 3 3 は、ステップ S T 3 4 で個別鍵であると特定された場合に、カード処理部 3 2 に装置識別データ I D M を要求する要求 I D M _ R E Q を出力する。

ステップ S T 3 9 :

カード処理部 3 2 は、ステップ S T 3 8 で入力した要求 I D M _ R E Q に応じて、ステップ S T 3 1 で I C 1 5 から入力した装置識別データ I D M を鍵管理部 3 3 に出力する。

ステップ S T 4 0 :

鍵管理部 3 3 は、鍵管理データ KMD から識別データ S I D に対応する鍵データ K O を読み出す。

そして、鍵管理部 33 は、鍵データ KO と、ステップ ST39 で入力した装置識別データ IDM と、ステップ ST32 で入力した識別データ SID とを鍵生成部 34 に出力する。

【0040】

ステップ ST41：

鍵生成部 34 は、図 7 を用いて説明した手順で、ステップ ST33 で入力した鍵データ等を用いて、個別鍵データ KI を生成する。

ステップ ST42：

鍵生成部 34 は、ステップ ST41 で入力した個別鍵データ KI を鍵管理部 33 に出力する。

【0041】

以上説明したように、カードシステム 1 では、図 6 を用いて説明したように、SAM12 において、認証プログラム 80 から鍵生成プログラム 81 に、識別データ SID1～SID3 を提供し、鍵生成プログラム 81 において識別データ SID2 のみを用いて個別鍵データ KI を生成する。そのため、認証プログラム 80 の開発者が鍵生成プログラム 81 に提供する識別データを基に鍵生成プログラム 81 における鍵生成アルゴリズムを推測することを困難にできる。

【0042】

また、SAM12 では、図 7 に示すようにファイアウォール FW1，FW2 が規定されているため、認証プログラム 80 が鍵生成プログラム 81 に不正にアクセスすることを防止でき、鍵生成プログラム 81 における鍵生成アルゴリズムをセキュアにできる。

【0043】

また、SAM12 では、認証プログラム 80 と鍵生成プログラム 81 とが関数 API1，API2 を介してデータ授受を行うこと以外完全に独立したプログラムであるため、認証プログラム 80 と鍵生成プログラム 81 との開発を異なる開発者が並行して進めることができる。

【0044】

また、SAM12 では、認証プログラム 80 および鍵生成プログラム 81 とは

独立して、鍵保存プログラム 82 を SAM12 の外部からダウンロードするように構成することで、鍵生成プログラム 81 に影響を与えることなく、鍵生成プログラム 81 を更新できる。例えば、所定のサービスを提供する事業者が鍵生成プログラム 81 を作製した場合に、鍵保存プログラム 82 を更新しても、当該事業者は鍵生成プログラム 81 を更新する必要がなく、負担を軽減できる。

【0045】

また、カードシステム 1 では、SAM12 は、IC15 との間でのサービス処理に先立って、IC15 から受けた IC カード 10 (IC15) に固有の装置識別データ IDM を基に、当該 IC15 に固有の個別鍵データ KI を生成し、個別鍵データ KI を基に IC15 との間で相互認証を行う。

そのため、複数の IC カード 10 のうち一部の IC カード 10 の個別鍵データ KI の秘匿性が失われた場合でも、他の IC カード 10 の個別鍵データの秘匿性は失われず、セキュリティを高めることができる。

【0046】

また、カードシステム 1 によれば、サービス等を識別する識別データ SID を IC15 から SAM12 に出力し、SAM12 において識別データ SID を基に個別鍵生成のアルゴリズムを切り換えるため、一部のアルゴリズムの秘匿性が失われた場合での、その他のアルゴリズムを基にした個別鍵データの秘匿性を保つことができる。

【0047】

また、カードシステム 1 によれば、サービス等を識別する識別データ SID を IC15 から SAM12 に出力し、SAM12 において識別データ SID を基に認証に用いる鍵データが個別鍵および固定鍵のいずれであるかを判断するため、IC15 では、認証に用いる鍵データが個別鍵および固定鍵のいずれであることを意識せずに処理を行うことができる。

【0048】

また、カードシステム 1 によれば、個別鍵および固定鍵に対応した処理の切り換えを鍵管理部 33 が行うため、カード処理部 32 は、認証に用いる鍵データが個別鍵および固定鍵のいずれであるかを特定せずに処理を行うことができる。そ

のため、カード処理部 32 の開発に伴う負担を軽減できると共に、個別鍵を用いた認証に関する情報がカード処理部 32 の開発者に漏れることを防止できる。

【0049】

また、カードシステム 1 によれば、鍵管理データ KMD の鍵特定データ KPD において、全ての鍵データについてその特性を固定鍵とすることで、固定鍵のみを用いるシステムと互換性をとることができる。

【0050】

また、カードシステム 1 によれば、カード処理部 32 の動作とは独立して、鍵管理部 33 において鍵管理データ KMD を基に個別鍵データに係わる処理を行うため、個別鍵データに関する情報を、カード処理部 32 のアプリケーションプログラムの開発者に知られないようにすることができる。すなわち、個別鍵データに関する情報を、鍵管理データ KMD、並びに個別鍵生成プログラム KPRG の設定・開発者のみに閉じることができ、高いセキュリティを実現できる。

【0051】

カードシステム 1 によれば、SAM12 は、上述したように装置識別データ IDM を基に個別鍵データを生成することで、全ての IC カード 10 の個別鍵データを記憶している必要がないため、小規模なメモリを用いて構成できる。

【0052】

本発明は上述した実施形態には限定されない。

また、上述した実施形態では、本発明の認証先として IC カード 10 の IC15 を例示したが、認証先はコンピュータなどであってもよい。

【0053】

【発明の効果】

本発明によれば、鍵生成手段における鍵データの生成手法を認証手段の開発者に秘密にできるデータ処理装置およびその方法を提供することができる。

また、本発明によれば、鍵生成のアルゴリズムを認証プログラムに対して秘匿にできるプログラムを提供することができる。

【図面の簡単な説明】

【図 1】

図 1 は、本発明の実施形態のカードシステムの構成図である。

【図 2】

図 2 は、図 1 に示す IC カードに内蔵された IC の構成図である。

【図 3】

図 3 は、図 1 に示す IC 内に規定された各種の鍵データを説明するための図である。

【図 4】

図 4 は、図 1 に示す SAM の機能ブロック図である。

【図 5】

図 5 は、図 4 に示す SAM の処理を説明するための図である。

【図 6】

図 6 は、図 5 に示す SAM のソフトウェア構成を説明するための図である。

【図 7】

図 7 は、図 6 に示す SAM 内のプログラムに規定されたファイアウォールを説明するための図である。

【図 8】

図 8 は、図 5 に示す SAM への鍵管理データの登録を説明するための図である。

【図 9】

図 9 は、図 5 に示す鍵生成部における個別鍵データの生成手順を説明するためのフローチャートである。

【図 10】

図 10 は、図 5 に示す SAM への鍵管理データの登録の手順を説明するためのフローチャートである。

【図 11】

図 11 は、図 5 に示す IC カードの IC と、SAM との間でサービスに関する処理を行う場合の動作例を説明するためのフローチャートである。

【図 12】

図 12 は、図 5 に示す IC カードの IC と、SAM との間でサービスに関する

処理を行う場合の動作例を説明するための図 11 の続きのフローチャートである。

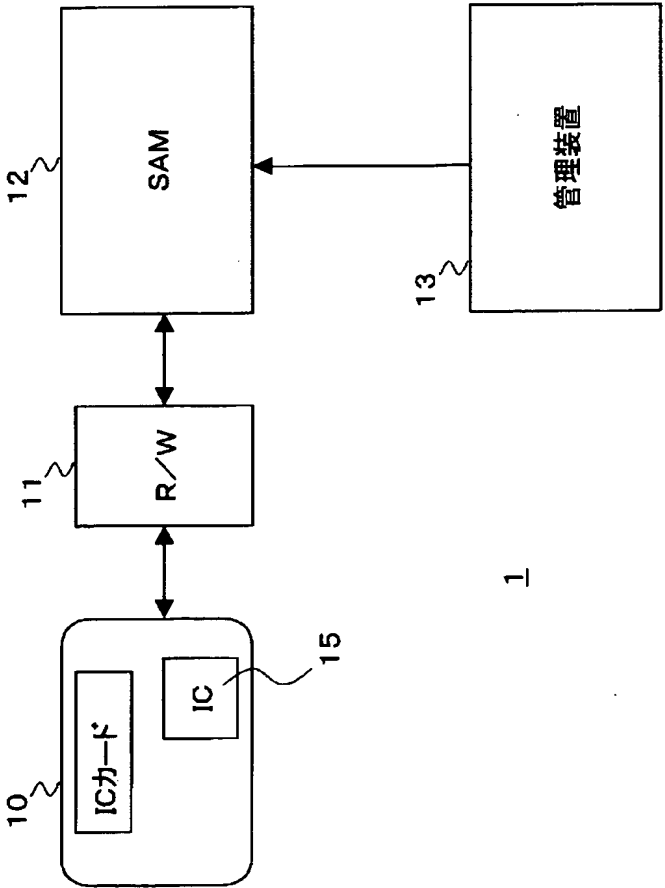
【符号の説明】

1…カードシステム、10…ICカード、11…R/W、12…SAM、13
円管理装置、15…IC、20…内部バス、21…インタフェース、22…メモ
リ、23…CPU、30…内部バス、31…インタフェース、32…カード処理
部、33…鍵管理部、34…鍵生成部、35…鍵保存部、80…認証プログラム
、81…鍵生成プログラム、82…鍵保存プログラム、FW1、FW2…ファイ
アウォール

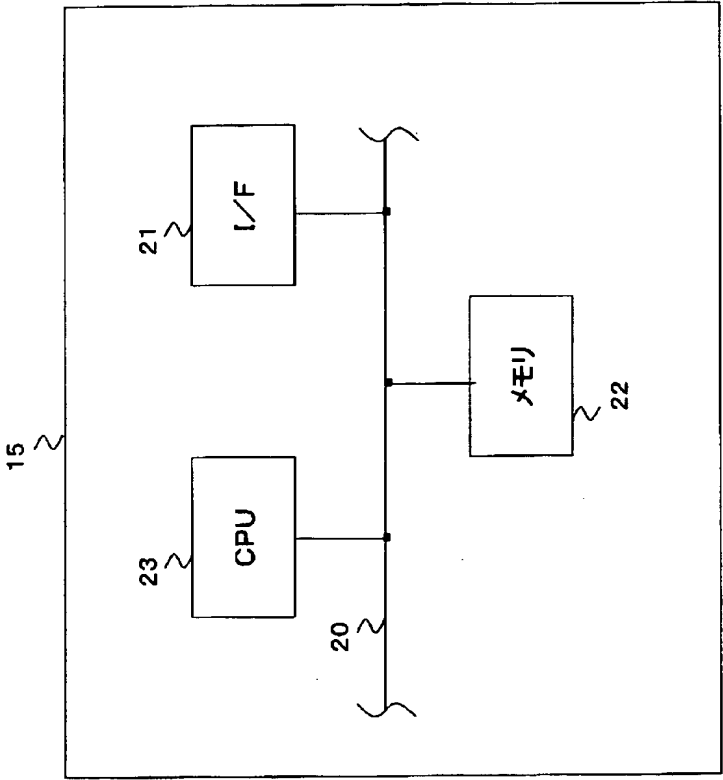
【書類名】

図面

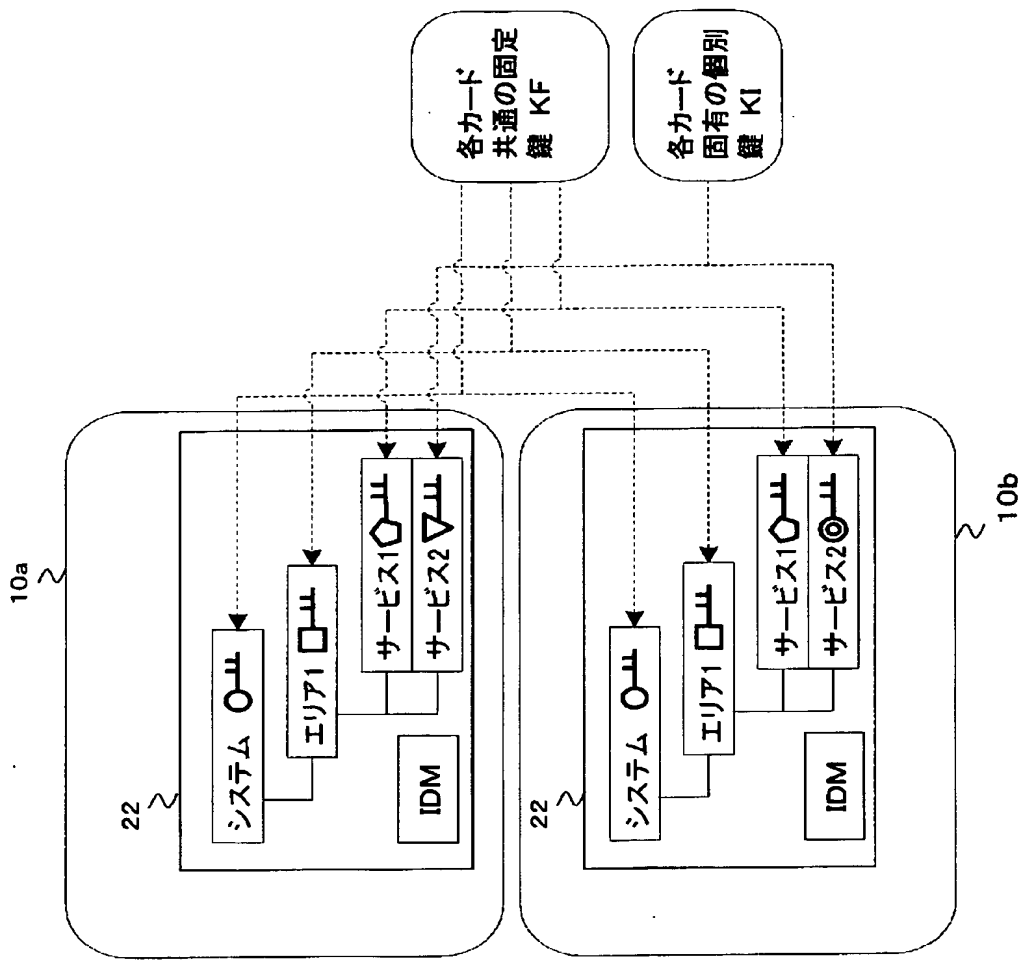
【図 1】



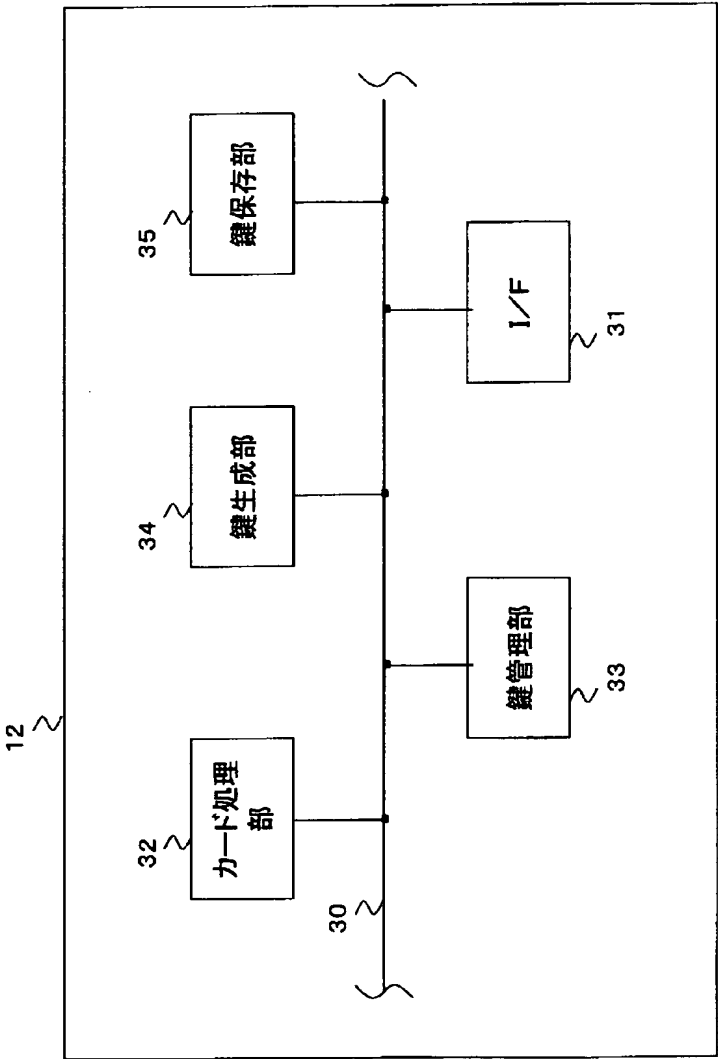
【図 2】



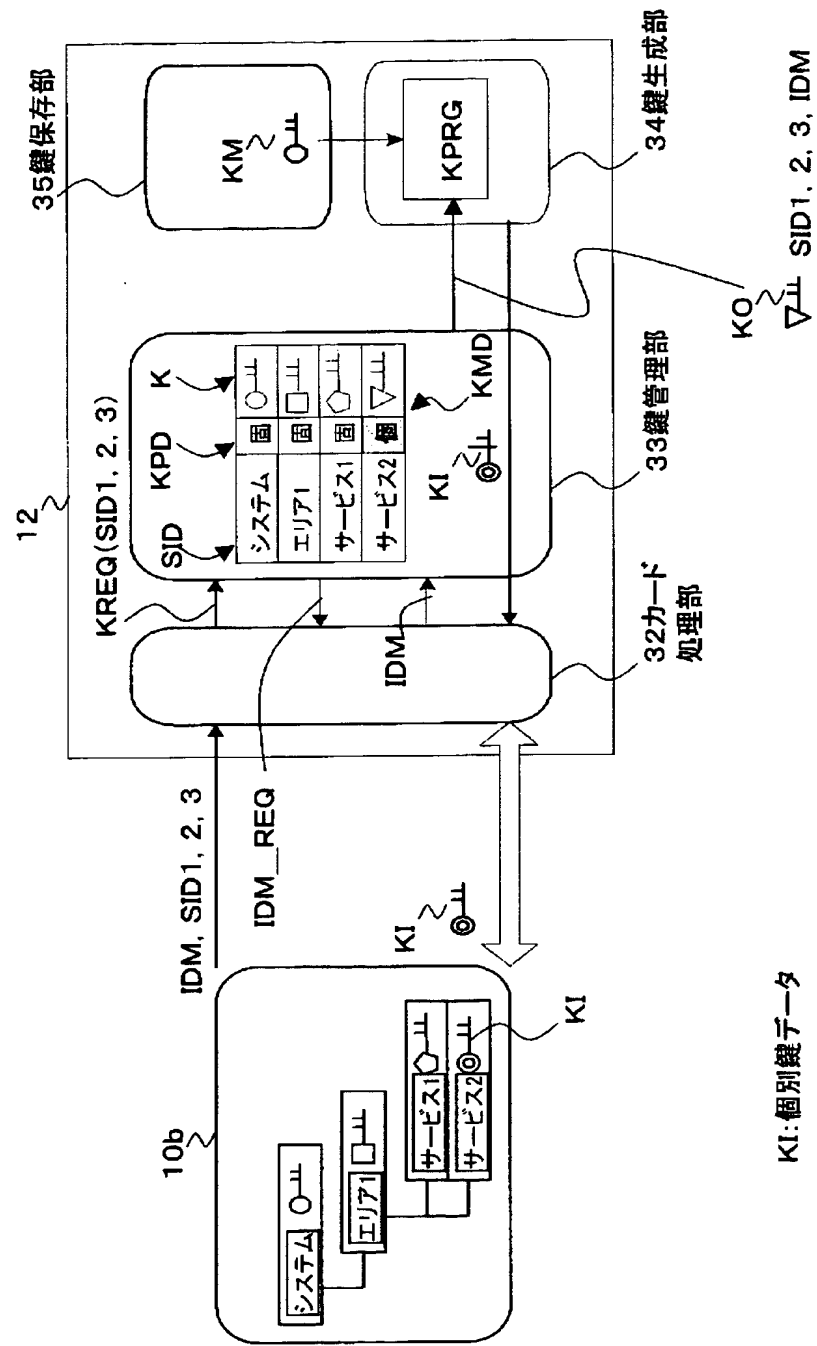
【図 3】



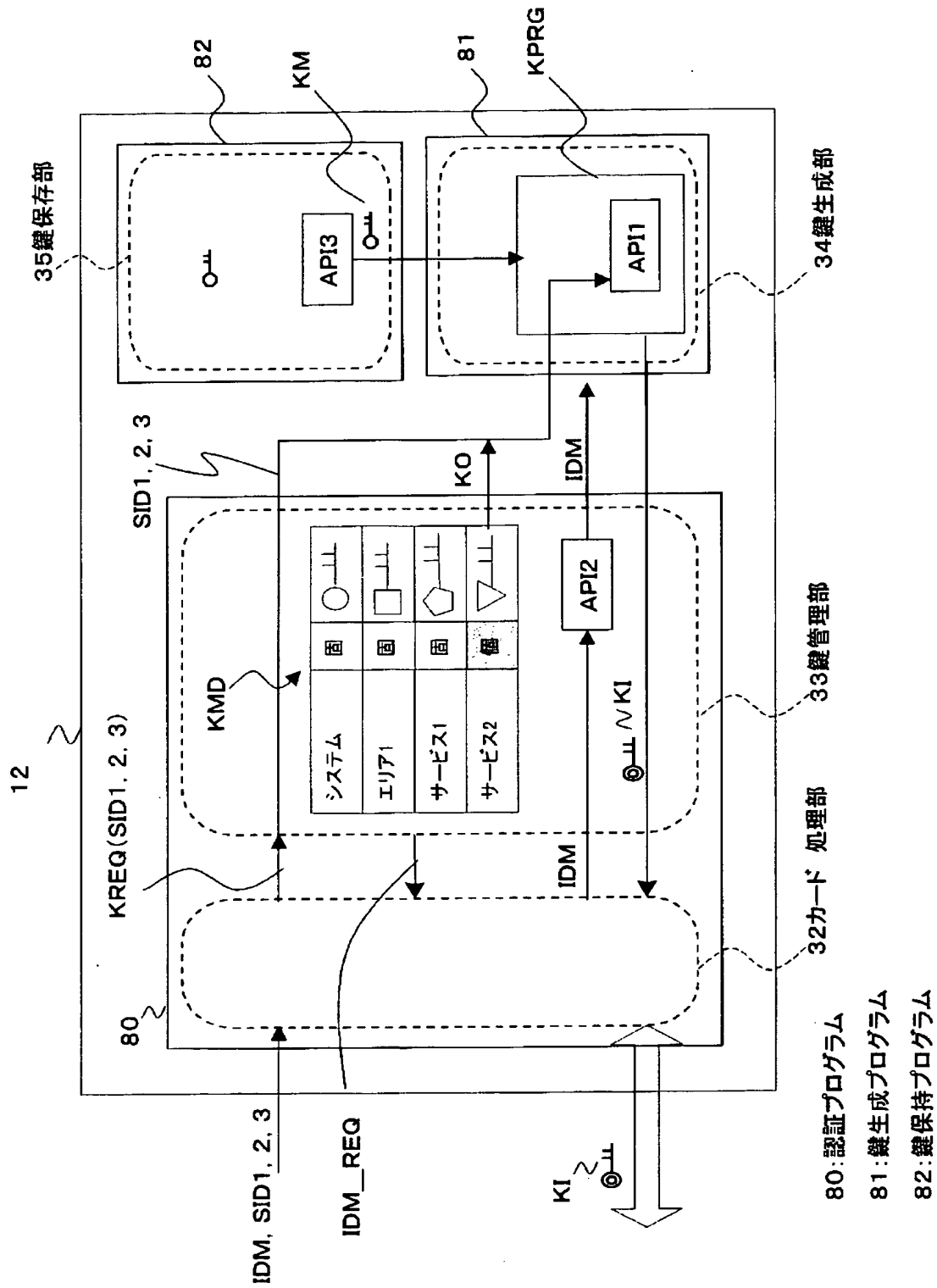
【図 4】



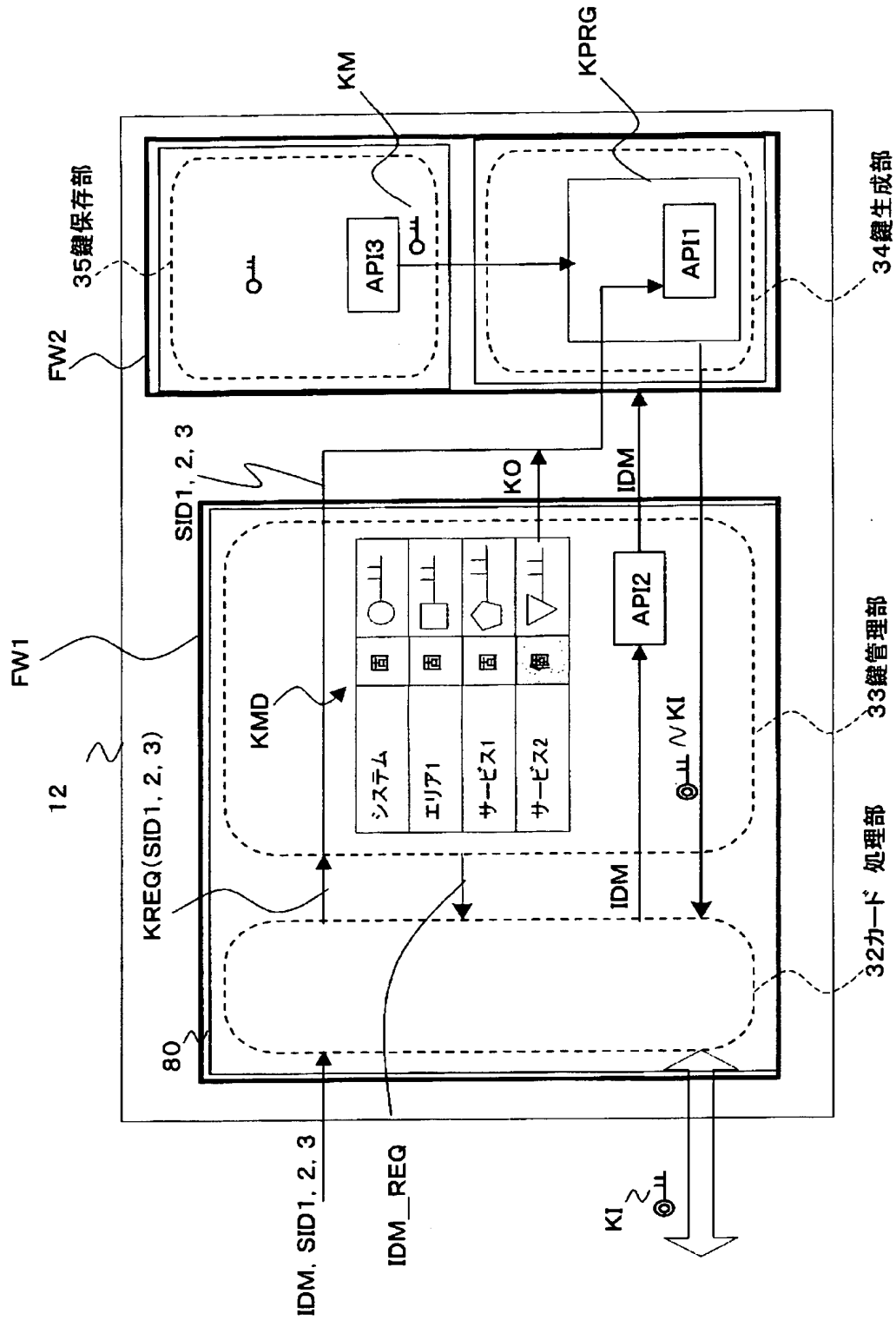
【図5】



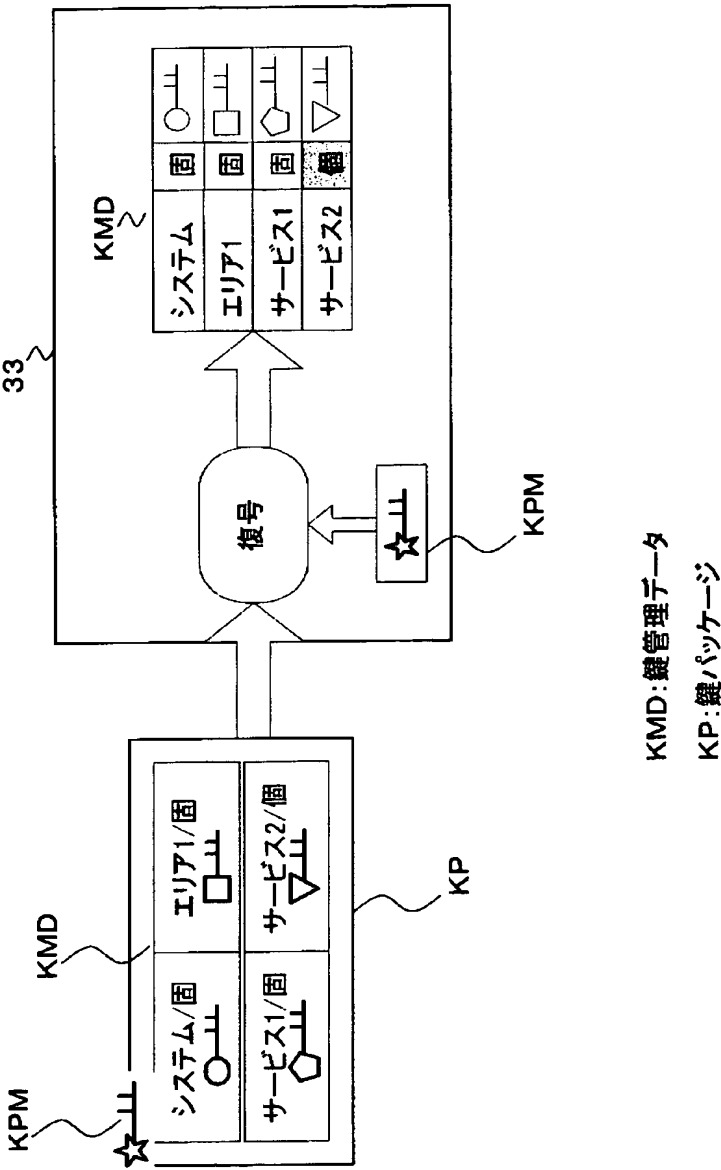
【図6】



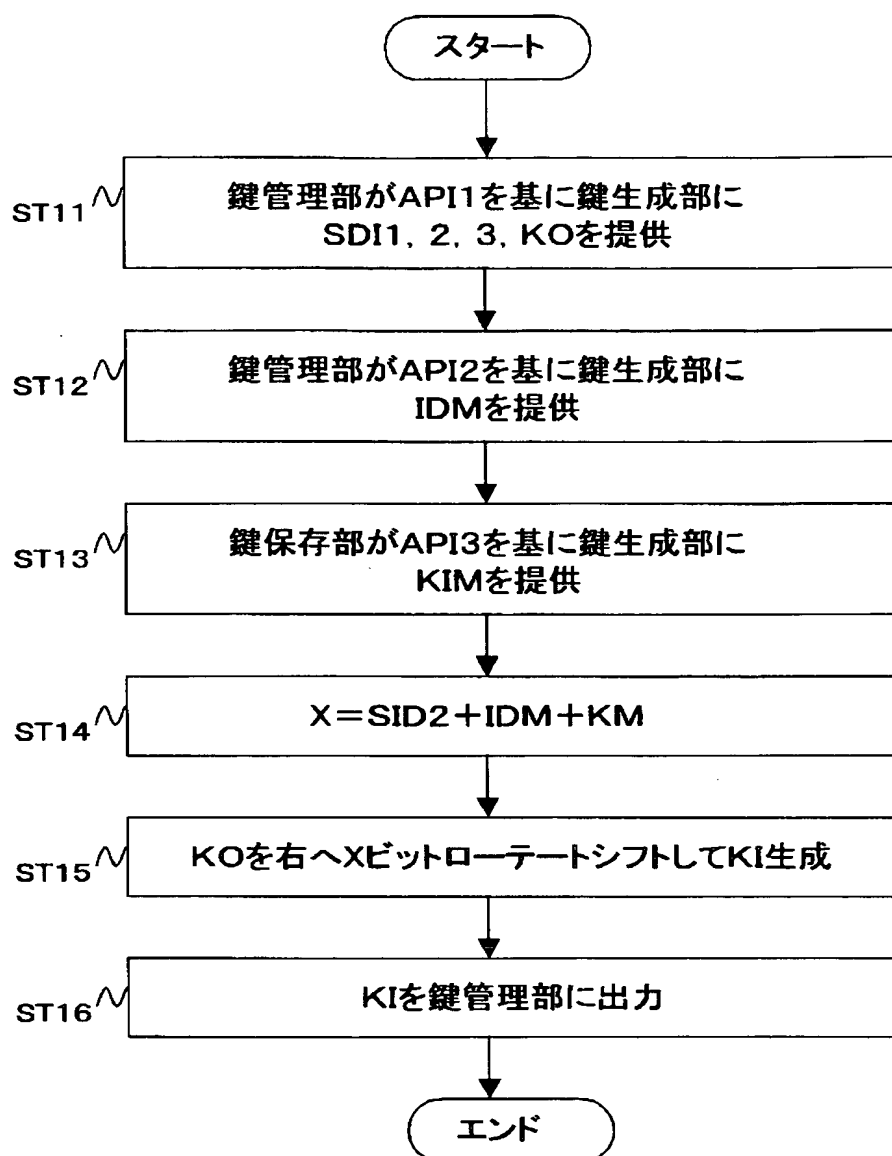
【図 7】



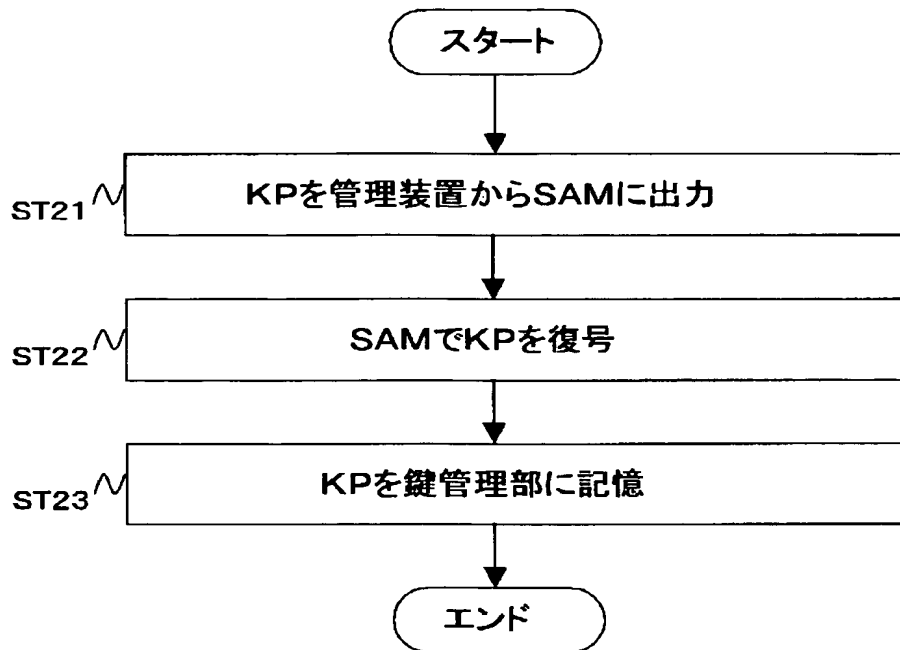
【図 8】



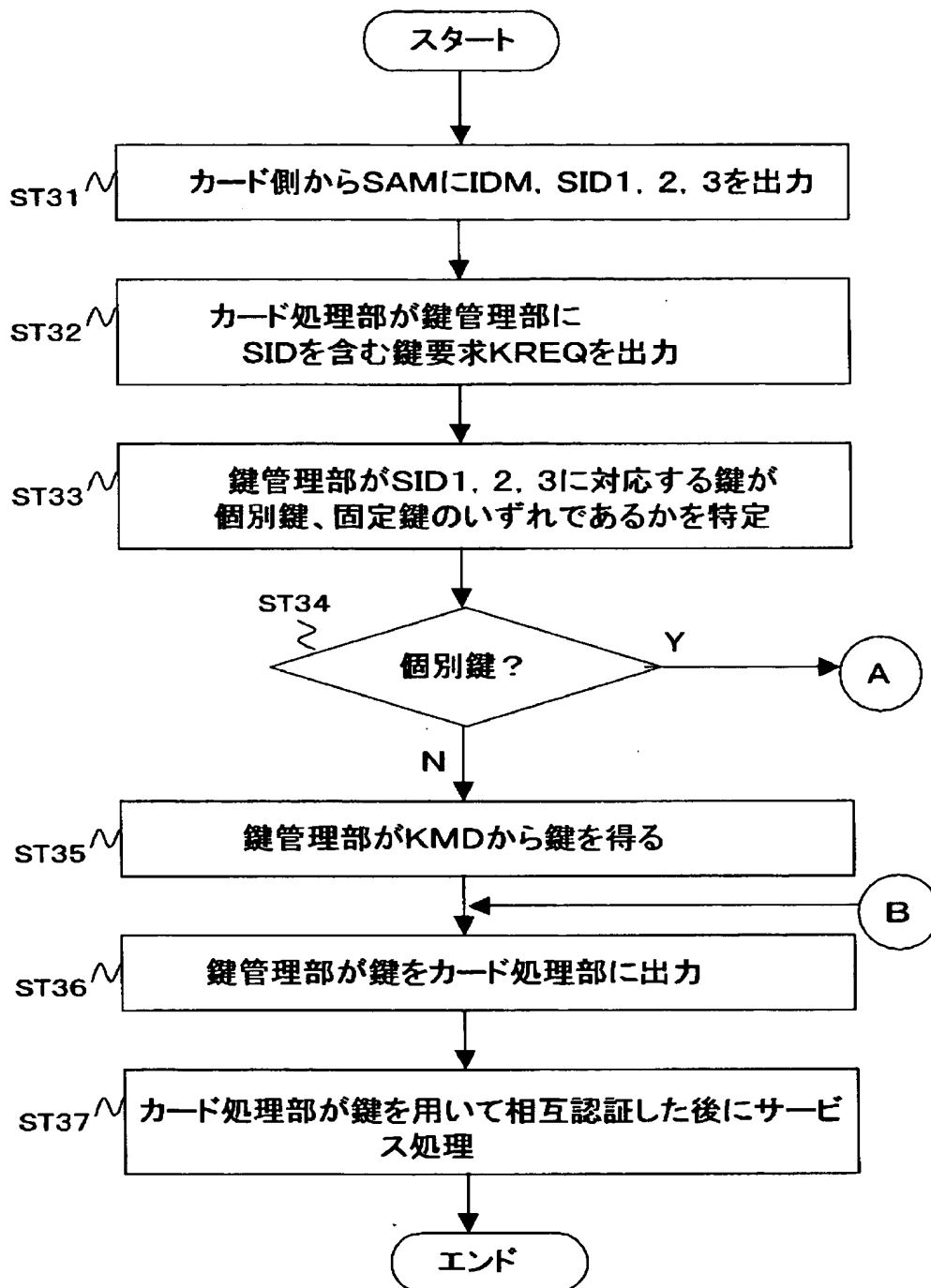
【図 9】



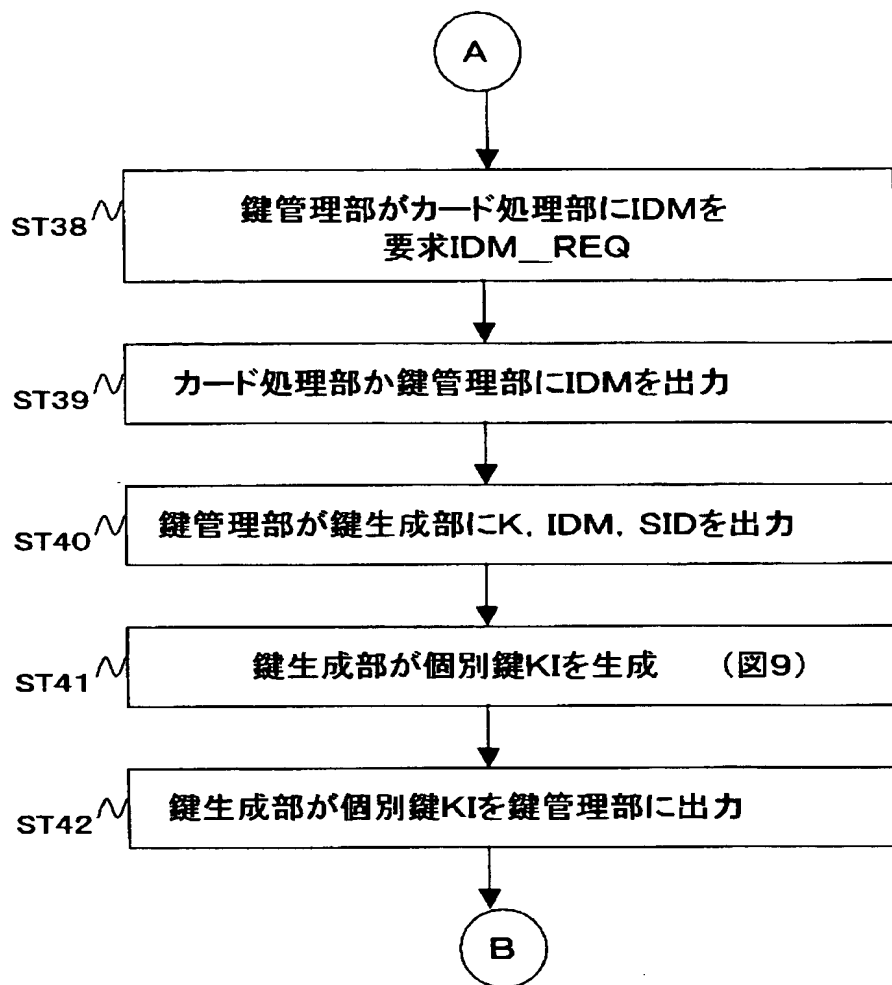
【図 10】



【図 11】



【図 12】



【書類名】 要約書

【要約】

【課題】 鍵生成手段における鍵データの生成手法を認証手段の開発者に秘密にできるデータ処理装置を提供する。

【解決手段】 認証プログラム 8 0 は、鍵生成プログラム 8 1 内の関数 A P I 1 を呼び出し、当該関数 A P I 1 の入力パラメータとして、I C カードの I C 5 から入力したサービス等の識別データ S I D 1, 2, 3 を代入する記述を有する。認証プログラム 8 0 を基にした当該コードの実行に応じて、所定のアドレスに書き込まれた識別データ S I D 1, 2, 3 を入力パラメータとして用いて鍵生成プログラム 8 1 が鍵生成を行う。

【選択図】 図 6

特願 2 0 0 3 - 0 7 0 3 0 1

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 2 1 8 5]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都品川区北品川 6 丁目 7 番 3 5 号

氏 名

ソニー株式会社